MARK OZZELLO (153989)
mark@ozzellolaw.com
17383 W Sunset Blvd, Ste A380
Pacific Palisades, CA 90272
Phone: (844) 774-2020

STEPHEN R. BASSER (121590)
sbasser@barrack.com
SAMUEL M. WARD (216562)
sward@barrack.com
BARRACK, RODOS & BACINE
One America Plaza
600 West Broadway, Suite 900
San Diego, CA 92101
Phone: (619) 230–0800
Fax: (619) 230–1874

Attorneys for Plaintiffs
(Additional Counsel for Plaintiff Appear on Signature Page)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

CARALYN TADA, CRAIG NOWINSKY, and LORI POBINER; individually and on behalf of all others similarly situated

Plaintiffs,

vs.

EQUIFAX, INC.

Defendants.

CLASS ACTION

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiffs Caralyn Tada, Craig Nowinsky, and Lori Pobiner ("Plaintiffs"), individually and on behalf of the classes defined herein, allege as follows against Equifax, Inc., ("Equifax"). Plaintiffs' allegations with respect to themselves are based on personal knowledge and, as to all other matters, on information and belief derived from a review of public documents and the investigation of Plaintiffs' counsel.

I. INTRODUCTION

1. On September 7, 2017, Equifax disclosed a staggering data breach impacting 143 million Americans (the "Equifax Data Breach"). Equifax's disclosure, which came more than five weeks after the Company claims to have learned of the breach, included an acknowledgement that the Equifax Data Breach occurred between mid-May and late July 2017. Information accessed by hackers included critical personal identifiable information ("PII") including names, Social Security Numbers, birth dates, addresses, and drivers license numbers. This PII is sufficient to allow identity thieves to wreak havoc on consumers through acts such as bank fraud and unauthorized opening of credit accounts. In addition to this PII, Equifax disclosed that the credit card numbers of approximately 209,000 persons were disclosed in the breach, and for an additional 182,000 persons documents containing PII were also accessed.

2. While acknowledging that it knew of the Equifax Data Breach for more than five weeks before disclosing it publicly, Equifax has failed to provide any explanation as to why it chose to wait to disclose the breach. Remarkably, even as the people impacted by the breach remained in the dark about the Equifax Data Breach, several high level executives at the Company, including Chief Financial Officer John Gamble, engaged in sales of Equifax stock, selling

approximately $1.8 million in stock in the days after the Company admits to have learned of the Equifax Data Breach.

3. The hackers who undertook the Equifax Data Breach did so by exploiting a web-based hack to access Equifax files. The nature of the hack suggests that Equifax failed to maintain even minimal data security standards despite the fact that it had previously been subjected to data breaches and despite its knowledge that, as a credit rating agency, the critical PII that it collects, stores, and maintains is a high value target to identity thieves and hackers.

4. Despite this knowledge, Equifax willfully, recklessly, and negligently failed to take adequate measures to protect PII, thus exposing approximately 143 million Americans to the threat of identity theft. Given the critical nature of the data accessed in the Equifax Data Breach, the threat to the people impacted by the breach is profound and long-lasting. As a result of the Equifax Data Breach, Plaintiffs and the members of the Class are subject to myriad harms including, but not limited to:

- Incurring costs associated with identity theft protection and monitoring services;
- Unauthorized use of PII;
- Monetary damages arising from fraudulent use of PII, including fraudulent access to bank accounts, credit cards, and other financial services;
- Damages arising from fees associated with such fraudulent use of PII, including late charges and delinquency fees;
- Adverse impact on credit scores and credit reports arising from unauthorized use of PII; and
- Costs associated with time spent addressing each of the above harms.

II. JURISDICTION AND VENUE

5. This Court has jurisdiction pursuant to 28 U.S.C. §§ 1331 as the action involves a federal question in that the action involves claims arising under a federal statute, the Fair Credit Reporting Act, 15 U.S.C. § 1681a.

6. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because members of the proposed Plaintiff Class are citizens of states different from Defendant's home state, and the aggregate amount in controversy exceeds in $5,000,000, exclusive of interests and costs.

7. This Court has personal jurisdiction over Equifax because Equifax regularly conducts business in California, has minimum contacts with California and maintains a place of business in this district.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because plaintiff Caralyn Tada resides in this district. In addition, Equifax conducts business in this district, a substantial part of the events or omissions giving rise to these claims occurred in this district, and Equifax has caused harm to Class members residing in this district.

III. PARTIES

9. Plaintiff Caralyn Tada is a resident of Redondo Beach, Los Angeles County, California. On September 7, 2017, Mrs. Tada learned that her PII had been accessed by unauthorized persons in the course of the Equifax Data Breach.

10. Craig Nowinsky is a resident of Great Neck, Nassau County, New York. Mr. Nowinsky is married to plaintiff Lori Pobiner. On September 7, 2017, Mr. Nowinsky learned that his PII had been accessed by unauthorized persons in the course of the Equifax Data Breach.

11. Lori Pobiner is a resident of Great Neck, Nassau County, New York. Mrs. Pobiner is married to plaintiff Craig Nowinsky. On September 7, 2017, Mrs. Pobiner learned that her PII had been accessed by unauthorized persons in the course of the Equifax Data Breach.

12. Equifax, Inc. is a Georgia corporation with offices throughout the United States. Describing itself as a "global information solutions company," Equifax maintains offices throughout the United States, including offices in Moorpark, California.

IV. STATEMENT OF FACTS

13. Equifax is one of the largest credit reporting agencies in the United States. According to its 2016 Annual Report, as of December 31, 2016, Equifax had 9,500 employees in 24 countries and generated annual operating revenue of more than $3.1 billion. Equifax generates this revenue through the collection and use of PII, providing, among other things, credit reports to businesses.

14. According to statements filed with the United States Securities Exchange Commission ("SEC"), Equifax accumulates a staggering array of PII on tens of millions of Americans for the purpose of enabling businesses "to make credit and service decisions, manage their portfolio risk, automate or outsource certain human resources, employment tax and payroll-related business processes, and develop marketing strategies concerning consumers and commercial enterprises." The Company acknowledges that this PII includes "credit, income, employment, asset, liquidity, net worth and spending activity, and business data, including credit and business demographics, that we obtain from a variety of sources, such as credit granting institutions, public record information, income and tax information primarily from large to mid-sized companies in the U.S., and survey-based marketing information."

15. Equifax acknowledges its responsibility to protect the PII that it collects, stores, and maintains and represents to consumers that it will do so. On its website, Equifax represents that it is subject to the Fair Credit Reporting Act ("FCRA"), and acknowledges that the FCRA, "among other things, restricts who has access to your sensitive credit information and how that information can be used."[1] Equifax further acknowledges that "[a] consumer reporting agency may not provide your credit report to any party that lacks a permissible purpose . . . ." *Id*. Despite its acknowledgment of its responsibility to protect the PII that it collects, stores, and maintains, and despite its representations regarding its responsibilities under the FCRA, Equifax failed to take reasonable and adequate steps to maintain the security of PII in its custody and control.

16. On September 7, 2017, Equifax published a statement acknowledging and, for the first time, publicly disclosing a massive data breach in which the PII of approximately 143 million Americans was accessed by unknown hackers.

Equifax Announces Cybersecurity Incident Involving Consumer Information

> September 7, 2017 — Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.
>
> The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to

[1] http://www.equifax.com/privacy/fcra, last visited on September 8, 2017.

determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.

Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers – all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. – 1:00 a.m. Eastern time.

In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries.

Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

> CEO Smith said, "I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will."

17. The Equifax announcement came more than five weeks after the Company first learned of the data breach. Equifax has provided no explanation as to why it waited weeks before warning people impacted by the breach that their critical PII had been accessed and stolen by unknown hackers. Remarkably, even while Equifax was failing to notify people impacted by the breach, thereby preventing the millions of impacted people from taking steps to protect themselves, several high level executives at the Company, including Chief Financial Officer John Gamble, engaged in sales of Equifax stock, selling approximately $1.8 million in stock in the days after the Company learned of the Equifax Data Breach – and before the Company's stock would inevitably fall once the massive Data Breach was announced.

A. Equifax Has Long Been Aware of the Risks of a Data Breach

18. Common sense dictates that credit bureaus, which maintain custody of critical PII for over a hundred million Americans, are a prime target of hackers who are either engaged in identity theft or who seek to profit by selling PII to identity thieves. In 2015, Experian, which, like Equifax, is one of the largest credit bureaus in the United States, announced that hackers had stolen the PII of fifteen million Americans. And, earlier this year, Equifax acknowledged a data breach at its TALX payroll subsidiary. In the TALX data breach, which was disclosed by Equifax in May 2017, hackers were able to steal data from W-2 tax forms through an exploit that went undetected for almost an entire year, from April 17, 2016 until March 29, 2017. The TALX data breach victimized

employees of several large employers that used TALX for payroll services, including Northrup Grumman, Allegis Group, and the University of Louisville.

19. Industry experts were critical of the security measures used by Equifax to protect the data maintained on TALX's electronic W-2 forms. Data security was reliant on a four digit PIN code and hackers were able to reset these PIN codes, thus accessing the W-2s. Avivah Litan, a fraud analyst with Gartner Inc., noted what an elementary failure the TALX data breach represented: "That's so 1990s," Litan said. "It's pretty unbelievable that a company like Equifax would only protect such sensitive data with just a PIN."[2] Litan continued by criticizing lax data protection practices at agencies such as Equifax, noting that "[t]here's about 500 percent more protection for credit card data right now than there is for identity data." *Id.*

20. Equifax's knowledge of the risks of PII data breaches is highlighted by the fact that Equifax profits off of consumer fears of such breaches. Equifax markets identity theft protection services directly to people who believe their PII has been involved in a data breach, telling them: "If you've recently been notified that your information was involved in a data breach, you likely have a lot of questions. We're here to help answer those questions and help you understand the steps you may take to help better protect your identity in the future."[3] The Equifax website counsels people whose PII has been hacked that "it is wise to consider taking advantage of the credit monitoring product, if it is offered." *Id.* And the very same page advertises Equifax's own "Equifax ID Patrol" and

[2] https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/, last visited on September 8, 2017.

[3] https://www.equifax.com/personal/identity-theft-protection, last visited on September 8, 2017.

"Equifax Complete Family Plan" products to people, assuring them that "a surprise-free future starts here." *Id.*

21. Equifax profited handsomely from consumer fears of identity theft and data breaches. As reported in Equifax's filings with the SEC, during the first six months of 2017 alone, Equifax earned more than $205 million in operating revenue from its "Global Consumer Solutions" segment, which includes revenue generated from "credit information, credit monitoring and identity theft protection products sold directly and indirectly to consumers via the internet and in various hard-copy formats. . . ."

22. Despite its knowledge of the risks of a data breach, and despite its knowledge of the critical nature of the PII that it collects, stores, and maintains, Equifax failed to take adequate and reasonably necessary steps to protect the PII in its possession.

23. The profound impact of the Equifax Data Breach has been highlighted by the cyber security industry. In a post titled, "Why the Equifax breach is very possibly the worst leak of personal info ever," *Ars Technica* writer Dan Goodin noted that "[c]onsumers' most sensitive data is now in the open and will remain so for years to come."[4] Goodin described the Equifax Data Breach as "very possibly []the most severe of all for a simple reason: the breath-taking amount of highly sensitive data it handed over to criminals. By providing full names, Social Security numbers, birth dates, addresses, and, in some cases, driver license numbers, it provided most of the information banks, insurance companies, and other businesses use to confirm consumers are who they claim to be. The theft, by criminals who exploited a security flaw on the Equifax website, opens

[4] https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/, last visited on September 9, 2017.

the troubling prospect the data is now in the hands of hostile governments, criminal gangs, or both and will remain so indefinitely." *Id.*

B. Equifax's Remediation Efforts are Insufficient and Harmful to Consumers

24. When Equifax disclosed the Equifax Data Breach, it indicated that it would provide remediation to consumers in the form of the Company's "TRUSTID" identity theft monitoring service. However, Equifax's announcement did not disclose that, buried deep in the TRUSTID terms of service is a clause requiring users to waive their right to bring suit against Equifax and/or to participate in any class action litigation undertaken against the Company. Instead, pursuant to the TRUSTID terms of service, consumers would be required to submit to arbitration. This broad waiver, hidden in the terms of service, serves to further victimize the millions of people who have already been harmed by Equifax's failure to adequately protect them and their critical and highly personal identity information.

25. On September 8, 2017, Equifax issued a statement indicating that "the arbitration clause and class action waiver included in the Equifax and TrustedID Premier terms of use does not apply to this cybersecurity incident." However, Equifax ***continues to include*** the arbitration clause and class action waiver in the TRUSTID terms of service, indicating that consumers who choose to use the TRUSTID identity theft monitoring services will be required to waive substantive rights with regard to that service.

26. In addition to requiring a waiver of the substantive rights of consumers, the Equifax offer of TRUSTID is good for just one year. Thereafter, people impacted by the Equifax Data Breach will be forced to choose between (a) paying for Equifax to protect them from the harms caused by the Equifax Data

Breach, (b) securing, and paying for, identity theft protection service from another provider, or (c) foregoing identity theft protection.

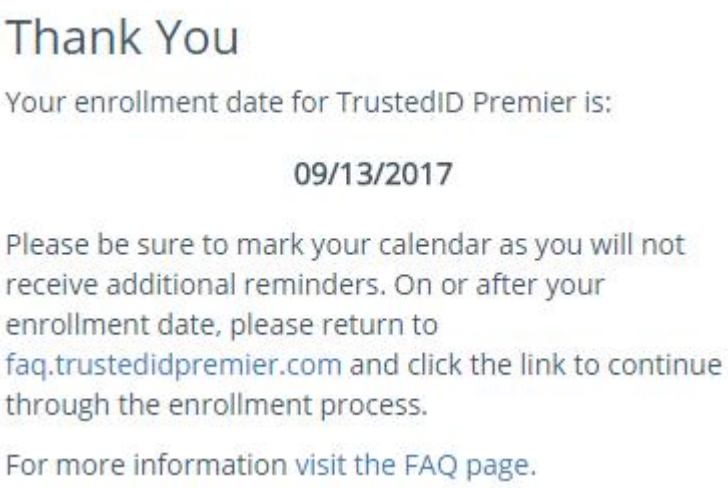
C. Equifax's Disclosure Points Consumers to an Unsecure and Unstable Website that Provides Unclear Information

27. As reported by online security analyst Jason Krebs, consumers attempting to access information regarding the Equifax Data Breach have met with significant problems, inconsistent directions, and error messages.

> [t]he Trustedid.com site Experian (sic) is promoting for free credit monitoring services was only intermittently available, likely because of the high volume of traffic following today's announcement.
>
> As many readers here have shared in the comments already, the site Equifax has available for people to see whether they were impacted by the breach may not actually tell you whether you were affected. When I entered the last six digits of my SSN and my last name, the site threw a "system unavailable" page, asking me to try again later.[5]
>
> In addition, the Equifax data breach site is providing consumers with confusing and unclear . . . with regard to their exposure.

As Krebs noted, "[w]hen I tried again later, I received a notice stating my enrollment date for TrustedID Premier is Sept. 13, 2017, but it asked me to return again on or after that date to enroll. ***The message implied but didn't say I was impacted*** (emphasis added).

[5] https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/, last visited on September 8, 2017.



28. On September 8, 2017, Krebs posted an update on the Equifax Data Breach in a post titled "Equifax Breach Response Turns Dumpster Fire."[6] Krebs described the website created by Equifax in response to the data breach, https://www.equifaxsecurity2017.com/, as "completely broken at best, and little more than a stalling tactic or sham at worst." *Id.* Krebs noted that the data breach website was itself insecure and, as a result, "the site was being flagged by various browsers as a phishing threat." *Id.* In addition, Krebs noted that the site continues to provide inconsistent information to consumers, "[i]n some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones." *Id.*

29. Cyber security expert Dan Goodin described Equifax's response to the data breach as "amateurish," noting that:

> The website www.equifaxsecurity2017.com/, which Equifax created to notify people of the breach, is highly problematic for a variety of reasons. It runs on a stock installation WordPress, a content management system that doesn't provide the enterprise-grade security required for a site that asks people to provide their last name and all but three digits of their Social Security number. The TLS certificate doesn't perform proper revocation checks. Worse still, the domain name isn't registered to Equifax, and its

[6] https://krebsonsecurity.com, last visited on September 9, 2017.

> format looks like precisely the kind of thing a criminal operation might use to steal people's details. It's no surprise that Cisco-owned Open DNS was blocking access to the site and warning it was a suspected phishing threat.[7]

Far from serving as remediation, Equifax's inadequate and haphazard response to the data breach is further indicia of its failure to take adequate and necessary steps to protect the PII of consumers.

D. Equifax's Remediation Effort is Limited to Provision of a Credit Protection Service Owned by Equifax

30. As set forth above, Equifax's proffer of TRUSTID to consumers who have been harmed as a result of Equifax's failure to protect their PII is entirely inadequate. Moreover, it is self-serving. TRUSTID is owned and operated by Equifax. TRUSTID and other identity theft monitoring services offered by the Company are a significant source of revenue, as set forth above, Indeed, such services generate tens, if not hundreds, of millions of dollars in revenue for Equifax every year. Remarkably, Equifax has positioned itself to profit from its failure to adequately protect the PII of consumers. Because of the critical nature of the PII accessed in the Equifax Data Breach, the single year of identify theft monitoring services offered by Equifax is insufficient. Consumers face a lifetime of threat arising from this data breach. Thus, many consumers are likely to continue using identity theft monitoring services such as TRUSTID for the foreseeable future.

---

[7] https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/, last visited on September 9, 2017.

V. CLASS ACTION ALLEGATIONS

31. Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed Class pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

32. The proposed nationwide class (the "Class") is defined as:

Nationwide Class

> All persons in the United States whose personal information was compromised or accessed by unauthorized individuals or entities in the data breach of Equifax disclosed by Equifax on September 7, 2017.

33. Plaintiffs also assert various claims on behalf of statewide classes, pursuant to Federal Rules of Civil Procedure 23. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2) and 23(b)(3) are met with respect to each of the statewide classes defined in the following paragraphs.

34. Plaintiffs claim on behalf of separate statewide classes that Equifax violated additional statutes of the states of California and New York as set forth below. These separate state classes are defined as follows:

California Class:

> All residents of California whose PII was compromised or accessed by unauthorized individuals or entities in the data breach of Equifax disclosed by Equifax on September 7, 2017.

New York Class:

> All residents of New York whose PII was compromised or accessed by unauthorized individuals or entities in the data breach of Equifax disclosed by Equifax on September 7, 2017.

35. Excluded from the Nationwide Class, the California Class, and the New York Class are: (1) Defendant, any entity or division in which Defendant has

a controlling interest, and its legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into subclasses or modified in any other way.

A. Numerosity and Ascertainability

36. Although the exact number of class members is uncertain and can be ascertained only through appropriate discovery, the number is great enough such that joinder is impracticable. Indeed, Equifax stated publicly that up to 143 million Americans' PII may have been breached. The disposition of the claims of these class members in a single action will provide substantial benefits to all parties and to the Court. Class members are readily identifiable from information and records in Equifax's possession, custody, or control.

B. Typicality

37. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all class members, had PII held by Equifax. Plaintiffs, like all class members, have been damaged by Equifax's conduct in that their PII has been compromised by Equifax's failure to fulfill its duties under the law. Further, the factual bases of Equifax's misconduct are common to all class members and represent a common thread of misconduct resulting in injury to all class members.

C. Adequate Representation

38. Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel with substantial experience in

prosecuting consumer and data breach class actions, and therefore Plaintiffs' counsel is also adequate under Rule 23.

39. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests adverse to those of the Class.

D. Predominance of Common Issues

40. There are numerous questions of law and fact common to Plaintiffs and the class members that predominate over any question affecting only individual class members. The answers to these common questions will advance resolution of the litigation as to all class members. These common legal and factual issues include:

a. Whether Equifax owed a duty to Plaintiffs and members of the Class to take reasonable measures to safeguard their personal information;

b. Whether Equifax knew or should have known that its cyber security systems were vulnerable to attack;

c. Whether Equifax's cyber security measures were reasonable in light of the substantial risk posed by hackers;

d. Whether Equifax's breach of a legal duty caused its cyber security systems to be compromised, resulting in the compromise of the PII of approximately 143 million Americans;

e. Whether Equifax owed a duty to Plaintiffs and members of the Class to provide timely and adequate notice of the Equifax data breach and the risks posed thereby, and whether Equifax's notice was, in fact, timely; and

f. Whether Plaintiffs and class members are entitled to recover actual damages, statutory damages, and/or punitive damages.

E. Superiority

41. Plaintiffs and Class members have all suffered and will continue to suffer harm and damages as a result of Equifax's unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

42. Absent a class action, most class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Further, without class litigation, class members will continue to incur damages and Equifax is likely to repeat its misconduct.

43. Class treatment of common questions of law and fact is also a superior method to multiple individual actions or piecemeal litigation in that class treatment will conserve the resources of the courts and the litigants, and will promote consistency and efficiency of adjudication.

F. Injunctive and Declaratory Relief

44. Defendant has, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class and California Subclass, making injunctive and declaratory relief appropriate as to the Class as a whole.

VI. CAUSES OF ACTION

COUNT I
VIOLATION OF THE FAIR CREDIT REPORTING ACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

45. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

46. Plaintiffs bring this Claim on behalf of the Nationwide Class

47. Pursuant to 15 U.S.C. §1681a(c), Plaintiffs and the members of the Class are "consumers," and thus entitled to the protections of the FCRA.

48. The Fair Credit Reporting Act, 15 U.S.C. § 1681a(f), defines a "consumer reporting agency" as:

> any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

49. Equifax is a consumer reporting agency under the FCRA because it engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and it does so for monetary fees.

50. The FCRA, 15 U.S.C. § 1681e(a), requires consumer reporting agencies like Equifax to "maintain reasonable procedures designed to…limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." Section 1681b does not permit consumer reporting agencies to disclose consumer reports to unauthorized individuals such as hackers and identity thieves.

51. Under the Fair Credit Reporting Act, Equifax had a duty to limit access to the consumer PII that it maintained in the course of its business. Equifax acknowledged this duty in the "FCRA Summary of Rights" maintained by Equifax at http://www.equifax.com/privacy/fcra.

52. The FCRA, 15 U.S.C. § 1681a(d)(1), defines a "consumer report" as:

> any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for--

(A) credit or insurance to be used primarily for personal, family, or household purposes;
(B) employment purposes; or
(C) any other purpose authorized under section 1681b of this title.

53. Equifax willfully and/or recklessly failed to maintain the reasonable procedures necessary for compliance under section 1681b of the FCRA, as evidenced by Equifax's prior exposure to a data breach, the heightened risk of data breaches faced by credit reporting agencies such as Equifax, and its self-professed knowledge of the importance of the ever-increasing risks posed to data security, as set forth herein.

54. Equifax's willful and/or reckless conduct as detailed herein caused Plaintiffs and members of the Class to be exposed to fraud and be harmed.

55. The FCRA, 15 U.S.C. § 1681n(a)(1)(A), allows for Plaintiffs and Class Members to recover "any actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000." Plaintiffs and Class Members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees, as set forth in 15 U.S.C. § 1681n(a)(2), (3).

COUNT II
VIOLATIONS OF CALIFORNIA CAL. CIV. CODE § 1798.81.5
(ON BEHALF OF PLAINTIFF TADA AND THE CALIFORNIA CLASS)

56. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

57. This cause of action is asserted by Plaintiff Caralyn Tada on behalf of herself and the California Class.

58. Pursuant to the California Civ. Code § 1798.81.5, businesses are required to take reasonable steps to and appropriate security measures to provide for the security and confidentiality of PII that they collect, store, and maintain.

59. Defendant had a duty to protect the PII of Plaintiffs and the members of the Nationwide and California Class and to prevent the unauthorized access to, and disclosure of, that PII.

60. Defendant's conduct violated Cal. Civ. Code § 1798.81.5.

61. As a result of Defendant's failure to meet its duties, Plaintiffs and members of the Nationwide Class and the California Class have been damaged.

62. Defendant's conduct was intentional, reckless, and/or negligent.

63. Plaintiffs and the members of the Nationwide Class and the California Class are entitled to recover damages and injunctive relief as a result of Defendants' wrongful conduct.

64. Plaintiffs and the members of the Nationwide Class and the California Class are entitled to punitive damages for Defendant's intentional, willful, and/or reckless conduct.

65. Plaintiffs and the members of the Nationwide Class and the California Class are entitled to attorneys' fees.

COUNT III
VIOLATIONS OF CALIFORNIA CAL. CIV. CODE § 1798.82
(ON BEHALF OF PLAINTIFF TADA AND THE CALIFORNIA CLASS)

66. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

67. This cause of action is asserted by Plaintiff Caralyn Tada on behalf of herself and the California Class.

68. Defendant was not authorized to disclose, transmit, or otherwise allow access to Plaintiff's and class members' PII to unauthorized persons.

69. As a result of Equifax's conduct, the PII of Plaintiff Tada and other members of the California Class was disclosed to or accessed by unauthorized persons.

70. Equifax had a duty to protect the PII of Plaintiff Tada and other members of the California Class and to prevent the unauthorized access and disclosure of that PII.

71. As a result of Equifax's conduct, the privacy of Plaintiff Tada and other members of the California Class was breached.

72. Pursuant to California Civil Code § 1798.82, Equifax is required to provide statutorily required notices and take other actions upon privacy violations and privacy or data breaches such as the violations and breaches alleged herein.

73. However Equifax failed to adhere to and comply with their statutory and other legal obligations provided under the relevant statutes including Cal. Civ. Code §§ 1798.82.

74. Equifax's conduct was intentional, reckless, and/or negligent.

75. The Equifax Data Breach proximately caused substantial damages to Plaintiff Tada and other members of the California Class.

COUNT IV
VIOLATIONs OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, *et seq*.
(ON BEHALF OF PLAINTIFF TADA AND THE CALIFORNIA CLASS)

76. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

77. This cause of action is asserted by Plaintiff Caralyn Tada on behalf of herself and the California Class..

78. The UCL prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising. Defendant violated (and continues to violate) the UCL through its business acts and practices as set forth herein, and specifically by failing to protect and safeguard the PII that the collected, maintained, and stored and by failing to timely notify Plaintiffs and

the members of the Nationwide Class and the California Class of the Equifax Data Breach. These business acts and practices were centered in, emanated from and were carried out, effectuated and perfected in the United States and from within the State of California.

79. Plaintiff Tada and the California Class were harmed by Equifax's aforementioned unlawful, unfair and fraudulent business acts and practices occurring in the State of California. As alleged herein, Plaintiff Tada and the California Class have been victimized by, and have suffered injury in fact and lost money or property as a result of, Experian's conduct associated with their failure to protect and safeguard the PII and their failure to timely notify Plaintiff Tada and the California Class of the Equifax data breach.

80. Equifax's actions and practices, as alleged in this Complaint, were unfair, deceptive, misleading and likely to deceive the consuming public within the meaning of the UCL.

81. As set forth herein, Equifax's wrongful actions resulted in harm to consumers that is ongoing. Equifax's acts constitute violations of the unfair prong of Cal. Bus. & Prof. Code § 17200 *et seq.*

82. There were reasonably available alternatives to further Equifax's legitimate business interests, other than the conduct described herein. As a result of its deception, Defendant has been able to reap unjust revenue and profit.

83. Unless restrained and enjoined, Defendant will continue to engage in the above-described conduct. Accordingly, injunctive relief is appropriate.

84. Plaintiff Tada, on behalf of herself and the other members of the California Class, seeks restitution and disgorgement of all money obtained from Plaintiff Tada and the California Class collected as a result of Equifax's misconduct and injunctive relief in the form of an order prohibiting Defendant from continuing such practices and requiring Defendant to engage in and

undertake corrective measures, and all such other and further relief this Court deems appropriate, consistent with Cal. Bus. & Prof. Code § 17203.

COUNT V
NEW YORK GENERAL BUSINESS LAW § 349
(ON BEHALF OF PLAINTIFFS CRAIG NOWINSKY AND LORI POBINER AND THE NEW YORK CLASS)

85. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

86. Plaintiffs Craig Nowinsky and Lori Pobiner bring this claim on behalf of themselves and the New York Class.

87. New York General Business Law § 349 ("GBL 349") makes unlawful deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in this state.

88. Defendant engaged in false and misleading marketing concerning the maintenance of PII that it collected, stored, and maintained. In the course of Equifax's business, trade, commerce or furnishing of any service, it willfully failed to disclose that its cyber security systems were inadequate to protect PII and that its cybersecurity policies and procedures were inadequately implemented.

89. Equifax failed to timely disclose the Breach to Plaintiffs and New York Class Members; indeed, Equifax knew of the Equifax Data Breach for more than five weeks before it was disclosed to the public.

90. Accordingly, Equifax made untrue, deceptive, and misleading representations of material facts and omitted and/or concealed material facts to Plaintiffs and the New York Class.

91. Equifax failed to provide adequate protection to the PII that it collected, stored, and maintained, resulting in the Breach.

92. Plaintiffs and the New York Class suffered injury caused by Equifax's affirmative statements, as well as its failure to disclose material information.

93. Plaintiffs and the New York Class also suffered injury owing to the diminution in value of their PII.

94. Pursuant to GBL 349, Plaintiffs and the New York Class are entitled to recover the greater of actual damages or $50. Because Equifax acted willfully or knowingly as described herein, Plaintiffs and the New York Class are entitled to recover three times their actual damages, up to $1,000.

COUNT VI
VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 899-AA (ON BEHALF OF PLAINTIFFS CRAIG NOWINSKY AND LORI POBINER AND THE NEW YORK CLASS

95. Plaintiffs repeat and reallege each and every one of the foregoing allegations as though fully set forth herein.

96. New York General Business Law § 899-aa requires businesses operating in New York State that maintain computerized data including personal and financial information, such as Equifax, to notify such consumers immediately upon discovering a breach of their systems if consumer information was or is reasonably believed to have been accessed or acquired by unauthorized persons.

97. As alleged herein, Equifax failed to notify Plaintiffs and the other members of the New York Class immediately upon the discovery of the Equifax Data Breach. Instead, Equifax waited more than five weeks before making a public disclosure disclosing the Equifax Data Breach and, as pleaded herein, that disclosure provided inconsistent information to consumers and the public regarding the data breach, in violation of General Business Law § 899-aa.

98. As a direct and proximate cause of Equifax's conduct as alleged herein, Plaintiffs and the members of the New York Class have suffered and continue to suffer harm and damages stemming from the Equifax Data Breach.

COUNT VII
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE THE NATIONWIDE CLASS)

99. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

100. Plaintiffs bring this Claim on behalf of the Nationwide Class.

101. In the course of its business, Equifax collected, stored, and maintained the non-public PII of Plaintiffs and members of the Class. Equifax therefore assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent disclosure of the PII, and to guard the PII from theft. Equifax's duty included a responsibility to implement a process by which it could detect and remedy a breach of its security systems in a reasonably expeditious period of time.

102. Equifax's duty arises from the common law, which is consistent across all states within the country.

103. Equifax breached its duty of care by failing to secure and safeguard the PII of Plaintiffs and the Class. Equifax negligently maintained systems that it knew were vulnerable to a security breach. Further, Equifax negligently stored consumer PII in a manner that rendered it subject to internet-based hacking, making it more likely a breach would net a greater (and more dangerous) breadth of PII.

104. Given the risks associated with data theft, Equifax also assumed a duty of care to promptly and fully notify and inform the people whose PII it collected, stored, and maintained that their personal information was compromised and/or stolen.

105. Equifax breached this duty of care when (a) it allowed its systems to be breached, and (b) it unreasonably waited over five weeks to notify the Class that its security systems had been breached. Equifax admits to having learned of the breach on July 29, 2017, yet said nothing to notify those affected for over five weeks. Equifax continues to breach this duty of care, by failing to share crucial information with Plaintiffs and the Class regarding the identity of people whose data was stolen and the specific nature of the data that was stolen.

106. Plaintiffs and the Class have suffered harm as a result of Equifax's breach. The PII of Plaintiffs and the Class have been exposed, subjecting each member of the Class to identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other varieties of identity fraud.

107. Plaintiffs and the Class have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Class have suffered and/or are reasonably likely to suffer theft of personal and health information; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of its myriad forms; and damages from the unconsented exposure of PII due to this breach.

COUNT VIII
NEGLIGENCE PER SE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

108. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

109. Plaintiffs bring this Claim on behalf of the Nationwide Class.

110. Under the Fair Credit Reporting Act, Equifax had a duty to limit access to the consumer PII that it maintained in the course of its business. Equifax

acknowledged this duty in the "FCRA Summary of Rights" maintained by Equifax at http://www.equifax.com/privacy/fcra.

111. Equifax violated the FCRA by failing to secure and safeguard the consumer PII that it maintained in the course of its business.

112. Equifax's failure to comply with the FCRA and regulations promulgated thereto constitutes negligence per se.

113. As a result of Equifax's negligence per se, Plaintiffs and the Class have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Class have suffered and/or are reasonably likely to suffer theft of PII; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of its myriad forms; and damages from the unconsented exposure of PII due to this breach.

COUNT IX
VIOLATION OF THE GEORGIA FAIR BUSINESS PRACTICES ACT
O.C.G.A. § 10-1-390, *ET SEQ.*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

114. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

115. Plaintiffs bring this Claim on behalf of the Nationwide Class.

116. In the course and scope of its business, Equifax's acts affect trans and commerce pursuant to O.C.G.A. § 10-1-392(28).

117. In the course and scope of its business, Equifax collects, stores, and maintains the PII of Plaintiffs and Class Members.

118. As alleged herein, Equifax engaged in unfair and/or deceptive acts or practices in the conduct of consumer transactions in violation of the Georgia Fair Business Practices Act (the "GFBPA").

119. Equifax knew, or should have known, that its data security practices and procedures were inadequate and insufficient to safeguard the PII of Plaintiffs and members of the Class.

120. Equifax knew, or should have known, that it was under a substantial and continuing threat from hackers and identity thieves.

121. As a direct and proximate cause of Equifax's violations of the GFBPA, Plaintiffs and members of the Class suffered damages including, but not limited to:

- Incurring costs associated with identity theft protection and monitoring services;
- Unauthorized use of PII;
- Monetary damages arising from fraudulent use of PII, including fraudulent access to bank accounts, credit cards, and other financial services;
- Damages arising from fees associated with such fraudulent use of PII, including late charges and delinquency fees;
- Adverse impact on credit scores and credit reports arising from unauthorized use of PII; and
- Costs associated with time spent addressing each of the above harms.

122. As a result of Equifax's violation of the GFBPA, Plaintiffs and the members of the Class are entitled to actual and consequential damages, attorneys' fees and costs, injunctive relief, and such other relief as the Court may deem appropriate.

REQUEST FOR RELIEF

Plaintiffs, on behalf of themselves and all others similarly situated, request that the Court enter judgment against Defendant, as follows:

1. An award to Plaintiffs and the Class of compensatory, direct, consequential, statutory, and incidental damages;

2. Injunctive relief requiring Defendant to refrain from demanding, as a condition of acceptance of identity theft monitoring services or any other remediation, a waiver of the right to sue and/or a waiver of the right to participate in a class action;

3. Injunctive relief requiring Defendant to implement measures that strengthen its data security protocols, provide for periodic audits of those protocols and adequately protect all members of the Class;

4. An award of attorneys' fees, costs, and expenses, as provided by law, or equity, or as otherwise available;

5. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

6. Such other or further relief as may be appropriate under the circumstances.

///

///

///

///

///

///

///

///

///

///

JURY TRIAL DEMANDED

Plaintiffs demand a jury trial as to all issues so triable.

DATED: September 11, 2017

Respectfully submitted,

BARRACK, RODOS & BACINE
STEPHEN R. BASSER (121590)
sbasser@barrack.com

/s/STEPHEN R. BASSER
STEPHEN R. BASSER

SAMUEL M. WARD (216562)
sward@barrack.com
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

MARK OZZELLO (153989)
mark@ozzellolaw.com
17383 W Sunset Blvd, Ste A380
Pacific Palisades, CA 90272
Telephone: (844) 774-2020
Facsimile: (310) 454-5970

JOHN G. EMERSON*
jemerson@emersonfirm.com
EMERSON SCOTT, LLP
830 Apollo Lane
Houston, TX 77058
Telephone: (281) 488-8854
Facsimile: (281) 488-8867

RONEN SARRAF*
ronen@sarrafgentile.com
JOSEPH GENTILE*
joseph@sarrafgentile.com
SARRAF GENTILE LLP
14 Bond Street, Suite 212
Great Neck, New York 11021

T 516.699.8890, ext. 12
F 516.699.8968

Attorneys for Plaintiffs
**Pro Hac Vice Applications Pending*